Cassandra Crossing/ Blockchain, Bitcoin, Smart Contract, NFT e Web 3.0

(502)—Un velocissimo excursus per avere almeno un'idea di cosa c'è dietro le buzzword più gettonate; se non ci credete provate a leggere.

Cassandra Crossing/ Blockchain, Bitcoin, Smart Contract, NFT e Web 3.0

Figure 1:

(502)—Un velocissimo excursus per avere almeno un'idea di cosa c'è dietro le buzzword più gettonate; se non ci credete provate a leggere.

11 maggio 2022—"*Buzzword*" è un termine inglese che indica quelle parole di moda che tutti usano, e che sembrano racchiudere un significato ben preciso e conosciuto. Chi le usa fa normalmente una bella figura, salvo che qualcuno gli ponga delle domande o chieda spiegazioni; in quel caso spesso la questione si complica.

Il titolo di oggi è non solo composto esclusivamente di *buzzword*, ma si tratta delle cinque più usate, e soprattutto abusate, degli ultimi due anni.

Cassandra, che saltuariamente ama porsi delle sfide, ha deciso di cimentarsi a scrivere un "*pezzo*" di **meno di mille parole**, che non solo le spieghi a grandi linee tutte e cinque, ma che soprattutto spieghi le loro relazioni; perché ce ne sono, ed anche molte!

Quindi, conscia della difficoltà, dopo aver invocato la protezione non solo di Zeus e del Manzoni, ma anche della signorina Pia, sua maestra di quinta elementare, e del professor Ghelardoni,

indimenticato docente di Analisi I in quella che fu la facoltà del geniale fratello di Fantozzi, inizierà ad intrattenere i suoi 24 intrepidi lettori proprio su queste. Cominciamo.

La **Blockchain** è una struttura informatica che, utilizzando la crittografia, permette di organizzare informazioni in modo da garantirne l'inalterabilità.
Possiamo rappresentarla come un grosso file, spesso condiviso su più computer, che è diviso in blocchi concatenati tra di loro, ciascuno dei quali contiene delle informazioni. Come una fila di scatoloni, ciascuno pieno di buste.
Il concatenamento crittografico dei blocchi permette di garantire che, se il primo blocco è autentico ed originale, tutti i seguenti lo sono, e permette a chiunque di aggiungere un nuovo blocco, rispettando le regole della particolare blockchain.

I **Bitcoin** sono una criptovaluta, cioè una moneta elettronica senza rapporti con il mondo materiale od altre valute.
E' realizzata mediante una blockchain pubblica e condivisa, utilizzata come un registro pubblico di notariato contabile.
Ogni blocco contiene un certo numero di registrazioni contabili, ciascuna delle quali registra il passaggio di Bitcoin da un "IBAN Bitcoin" (indirizzo Bitcoin) ad un altro.
Chiunque può utilizzare un "conto Bitcoin" (wallet) per scambiare Bitcoin con altri possessori di wallet, chiedendo alla rete dei server di autenticare una sua registrazione contabile di trasferimento di denaro.

A differenza di quelli bancari, ad un singolo "conto Bitcoin" (wallet) corrispondono infiniti "IBAN" Bitcoin.

Esistono dei "volontari", dotati di server con enormi capacità di calcolo, che prendono alcune delle registrazioni contabili, richieste ma non ancora registrate (buste), le inseriscono in un blocco temporaneo della blockchain (scatolone) e cercano di "agganciarlo" alla blockchain (fila di scatoloni), eseguendo un complicatissimo calcolo matematico (che per inciso consuma moltissima energia elettrica).

Il primo che ci riesce vince, "aggancia" il nuovo blocco alla blockchain e lo invia a tutti i server.
Tutti gli altri, che stavano tentando di fare la stessa cosa ma hanno "perso", buttano via il lavoro fatto e ricominciano da capo con un nuovo blocco, contenente nuove registrazioni contabili.
Chi ha "vinto", e creato il nuovo blocco della blockchain, riceve in premio un certo numero fisso di Bitcoin "creati" dal nulla ("minati") più l'ammontare di tutte le "commissioni", fatte di Bitcoin già esistenti, contenute nelle richieste di registrazioni contabili che ha autenticato.
Se la sua bolletta dell'energia elettrica è più bassa del valore dei Bitcoin che riceve, guadagna soldi.

Gli **Smart Contract** sono una forma di "*criptovaluta intelligente*", realizzata tramite una tecnologia blockchain, e sopra un criptovaluta esistente.
La prima criptovaluta su cui sono stati realizzati è *Ethereum*, che permette di realizzare una "*registrazione contabile intelligente*" che scambi in automatico degli "*Ether*" (che sono le monete della rete Ethereum) al verificarsi di certe condizioni, ad esempio al passare di una certa data, o se qualcuno inserisce un certo altro pagamento nella blockchain.
Il contratto intelligente viene "scritto" in un apposito linguaggio di programmazione ed "eseguito" da tutti i server che formano la rete Ethereum.
Una banca potrebbe ad esempio concedere un "*mutuo intelligente*" in Ethereum, inserendone l'ammontare in Ether nella rete Ethereum, con "attaccato" un contratto di mutuo scritto come "smart contract". L'ammontare in Ether del mutuo andrebbe automaticamente a chi l'ha richiesto, e gli rimarrebbe se pagasse regolarmente in Ether certe rate di rimborso a certe date, mentre gli verrebbe tolto se non lo facesse.

La rete Ethereum tra l'altro consuma molta meno energia di Bitcoin perché la sua blockchain funziona in maniera diversa.

Gli **NFT, (Non-Fungible Tokens—Gettoni non riproducibili)**, sono "*registrazioni di proprietà*" di un certo file, realizzate utilizzando una blockchain.
I certificati di proprietà possono essere creati e scambiati sulla rete Ethereum, o su altre reti di criptovalute, come *smart contract*.
I certificati normalmente non contengono il file di cui garantiscono la proprietà, ma solo una sua "impronta digitale".

I file possono essere facce di scimmiette, l'audio della lettura di un romanzo di Baricco, una scansione della Gioconda o la formula della Coca-Cola. Inspiegabilmente, le prime sono le più popolari e le più scambiate.

La "proprietà" che questi certificati "garantiscono" non impedisce a nessuno di copiare il file originale, che è normalmente "off-chain", cioè non si trova dentro la blockchain.
La "proprietà" ed il "valore" eventualmente associati ad un dato NFT sono frutto di convenzioni ed accordi tra i partecipanti agli scambi.
Se l'NFT "gira" sulla rete Ethereum, il suo valore è in Ether, anche se normalmente, parlandone, lo si converte in Euro o Dollari al cambio corrente.

Il **Web 3.0** è una futura implementazione di siti web in cui la vera moneta, normalmente regalata dagli utenti alle grandi aziende come Google o Meta, che è il tempo e l'attenzione che gli utenti dedicano ad un certo sito, viene invece "creata", posseduta e scambiata secondo i metodi sopra illustrati.
Nel Web 3.0 ogni utente possiederebbe delle criptovalute o degli NFT che guadagnerebbe visitando siti web, usando un social o facendo altre attività in Internet.
Potrebbe successivamente spenderli in cambio di oggetti o servizi.
Le grandi aziende stabilirebbero le regole del gioco, gestirebbero i tavoli di questi casinò e deciderebbero, spontaneamente e generosamente, di "spartire la torta" con i propri utenti, "pagandoli" invece di limitarsi a "regalargli" dei servizi come fanno oggi.
Tutti felici e contenti.
Ovviamente senza rivendita di dati personali, senza tecnocontrollo e senza danni derivanti dalla cessione di infiniti dati personali.

Ah, e la Luna è fatta di formaggio verde…

Finito! Sono 871 parole. Missione compiuta.

E se il pezzo fosse stato per voi interessante, potreste persino decidere di scrivere una riga di incoraggiamento a Cassandra.

Scrivere a Cassandra—twittare a Cassandra
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on May 12, 2022.

Canonical link